Cartilha de Segurança para Internet

16 de outubro de 2000

Resumo

Esta cartilha destina-se aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet. Como tais usuários não possuem conhecimentos dos termos técnicos normalmente empregados pelos profissionais da área de informática, usou-se uma linguagem não-técnica neste texto.

A idéia desta cartilha é dar ao usuário iniciante uma visão geral dos conceitos mais básicos de segurança.

Sumário

1 Introdução

Sabemos que no mundo real não existem sistemas totalmente seguros e o mundo virtual segue o mesmo preceito. Por maior que seja a proteção adotada, estaremos sempre sujeitos a invasões, roubos e ataques. Então é importante que conheçamos o perigo e saibamos como nos proteger.

Atualmente já nos utilizamos a Internet para realizar diversos serviços corriqueiros, como compras, serviços bancários, investimentos, além de negócios ou troca de informações confidenciais via *e-mail*.

Grande parte dos problemas ocorrem por puro desconhecimento dos procedimentos básicos de segurança por parte dos usuários. Saber como agir em caso de problemas, também poderá ajudar, e muito, nas investigações policiais dos crimes virtuais.

Mas, como tudo isso pode ser feito de maneira segura? Para fornecer informações de como utilizar de maneira segura os serviços da Internet é que esta cartilha foi criada.

2 Senhas

Uma senha ou *password* na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, a senha garante que determinado indivíduo que utiliza de um serviço é ele mesmo. Se você fornece sua senha para uma outra pessoa, esta poderá utilizar a senha para se passar por você na Internet e, dependendo do caso, o estrago poderá ser grande[1]. Portanto, a senha merece consideração especial, afinal, ela é de sua inteira responsabilidade.

2.1 Como escolher uma boa senha?

Uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar.

[1] Ou muito caro, visto que a pessoa que possuir a sua senha poderá usar seu provedor e quem pagará a conta (horas de uso) será você.

Normalmente os sistemas diferenciam letras maiúsculas das minúsculas[2] o que já ajuda na composição da senha.

Claro que o seu sobrenome, números de documentos, placas de carros, números de telefones e datas deverão estar fora de sua lista de senhas. Pois esses dados são muito fáceis de se obter e qualquer criminoso tentaria utilizar este tipo de informações para se autenticar como você.

Existem várias regras de criação de senhas que você pode utilizar, uma regra de ouro para a escolha de uma boa senha é: jamais utilize como senha palavras que façam parte de dicionários (de qualquer língua, deste ou de outros planetas[3]).

O que fazer então? Fácil perceber, quanto mais "bagunçada" a senha melhor, pois mais difícil será descobri-la. Assim tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

Por exemplo: usando a frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a seguinte senha "BqnsepC". Mas só tem 7 caracteres! Precisamos de pelo menos mais um para completar o mínimo de 8 caracteres. Assim a senha gerada fica: "!BqnsepC"[4]. Note que a senha gerada é bem "bagunçada", tem 8 caracteres com letras minúsculas e maiúsculas e um sinal de pontuação colocado em um lugar pouco convencional. Senhas geradas desta maneira são fáceis de lembrar e são normalmente difíceis de serem descobertas. Usando a última letra de cada palavra da frase da senha anterior, por exemplo, não gera uma senha muito elegante ("aoeeaoo") e há repetição de caracteres.

2.2 Com que freqüência devo mudar minha senha?

A regra básica é trocá-la pelo menos a cada dois ou três meses[5]. Existem páginas nos provedores que facilitam a troca da senha, e estão lá para serem utilizadas. Trocando-a regularmente você garante a integridade da mesma. Caso não encontre o serviço de troca de senha no *site* de seu provedor, entre em contato com o serviço de suporte, mas não aceite que a mudança da senha seja feita por funcionários. A alteração da senha **sempre** deve ser feita pelo próprio dono!

Lembrando: **a senha é importantíssima e mantê-la em segredo é a sua segurança!**

2.3 Quantas senhas diferentes devo usar?

Várias, uma para cada *site* de *e-mail* gratuito, uma para seu provedor, uma para o banco, uma para... Imagine o estrago que uma pessoa pode fazer se descobrir

[2]Cuidado, PeDrO e pEdRo são senhas diferentes mas fáceis de descobrir.

[3]Existem softwares que tentam descobrir a senha chutando combinações de palavras e testando. Estes softwares geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.).

[4]Esta senha deixou de ser uma senha boa, pois todos que lerão esta cartilha a conhecerão.

[5]Paranóicos e militares costumam trocá-la mensalmente ou semanalmente.

uma de suas senhas, e se esta senha que você usa é igual para todo os sites e serviços que você utiliza, com certeza o estrago vai ser muito maior.

3 Problemas Usuais de Segurança

3.1 Engenharia Social

O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança. Quem está mal intencionado geralmente utiliza telefone, *e-mails* ou salas de bate-papo para obter as informações que necessita.

Por exemplo: Algum desconhecido liga para a sua casa e se diz do suporte técnico do seu provedor. Nesta ligação ele te convence de que sua conexão com a Internet está problemática e pede sua senha para corrigir o problema.

Como sempre, o bom senso nestes casos é tudo. Duvide desse tipo de abordagem e contate o provedor caso algum técnico ligue para sua casa pedindo dados confidenciais a seu respeito (senhas, números de cartões, etc.) avisando-o do ocorrido.

Outro caso típico são *sites* desconhecidos que prometem "horas grátis" em seu provedor caso você passe o seu *username* e a sua senha para eles. É claro que eles utilizarão estes dados para conseguir "horas grátis", não para você mas para eles.

3.2 Cavalos de Tróia

Conta a mitologia grega, que há muito tempo atrás, houve uma guerra entre as cidades de Atenas e de Tróia. Como Tróia era extremamente fortificada, os militares gregos a consideravam inexpugnável. Para dominá-la os gregos construíram uma enorme estátua de madeira na forma de um cavalo e deram de presente para os troianos que a aceitaram de bom grado. O problema é que o cavalo foi recheado com centenas de soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos soldados gregos e a dominação de Tróia. Daí surgiram os termos *Presente de Grego* e *Cavalo de Tróia*.

Em tempos modernos o cavalo virou um programa e a cidade o seu computador. Conhecidos como *Cavalos de Tróia* ou *Trojan Horses* estes programas são construídos de tal maneira que, uma vez instalados nos computadores, abrem portas em seus micros, tornando possível o roubo de informações (arquivos, senhas, etc.).

3.2.1 Como meu computador pode ser infectado por um Cavalo de Tróia?

Normalmente você receberá o Cavalo de Tróia como presente (de grego). Ele pode ser dado a você de várias maneiras, mas na maioria das vezes ele vem anexado a algum *e-mail*. Estes *e-mails* vêm acompanhados de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Não se deixe enganar. A

melhor política é **nunca** abrir um arquivo anexado, principalmente se o remetente for desconhecido.

Programas piratas, adquiridos pela rede, poderão conter Cavalos de Tróia, assim, evite a instalação de programas de procedência desconhecida ou duvidosa.

3.2.2 O que um Cavalo de Tróia pode fazer em meu computador?

O Cavalo de Tróia, na maioria das vezes, vai possibilitar aos *hackers* o controle total da sua máquina. Ele poderá ver e copiar todos os seus arquivos, descobrir todas as senhas que você digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado. Este processo é chamado de **invasão**.

3.2.3 O *hacker* poderá me invadir se o computador não estiver conectado à Internet?

Não, o Cavalo de Tróia somente poderá ser utilizado se o computador estiver conectado à Internet. Os *hackers* somente invadem computadores quando eles estão conectados.

3.2.4 O computador pode ser infectado por um Cavalo de Tróia sem que se perceba?

Sim, com certeza! Essa é a idéia do Cavalo de Tróia, entrar em silêncio para que você não perceba e quando você descobrir ser tarde demais.

3.2.5 Como posso saber se o computador está infectado?

Os programas anti-vírus normalmente detectam os programas Cavalos de Tróia e tratam de eliminá-los como se fossem Vírus. As atualizações dos Anti-Vírus possibilitam a detecção dos Cavalos de Tróia mais recentes.

3.2.6 Como proteger o computador dos Cavalos de Tróia?

A maioria dos bons programas de anti-vírus são capazes de detectar e eliminar estes programas. Mesmo assim a proteção é parcial, uma vez que os Cavalos de Tróia mais novos poderão passar despercebidos. O ideal é nunca abrir documentos anexados aos *e-mails*.

Existem ainda programas de *Firewall* pessoal que podem ser utilizados para barrar as conexões dos *hackers* com os Cavalos de Tróia que possam estar instalados em seu computador. Tais programas não eliminam os Cavalos de Tróia, mas bloqueiam seu funcionamento.

3.3 *Backdoors*

Existe uma confusão entre o que é um *Backdoor* e um Cavalo de Tróia, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um Cavalo de Tróia é um programa que cria deliberadamente um *Backdoor* em seu computador. Programas que usam a Internet e que são de uso corriqueiro, como *Browsers*, programas de *e-mail*, *ICQ* ou *IRC* podem possuir *Backdoors*.

Os *Backdoors* são abertos devido a defeitos de fabricação ou falhas no projeto dos programas, isto pode acontecer tanto acidentalmente ou ser introduzido ao programa propositalmente. Como exemplo: versões antigas do *ICQ* possuem defeito que abre um *Backdoor* que permite ao *hacker* derrubar a conexão do programa com o servidor, fazendo que ele pare de funcionar.

3.3.1 Como se prevenir dos *Backdoors*?

A maneira mais correta é **sempre** atualizar as versões dos programas instalados em seu computador. É de responsabilidade do fabricante do software avisar aos usuários e prover uma nova versão corrigida do programa quando é descoberto um *Backdoor* no mesmo.

A dica é sempre visitar os *sites* dos fabricantes de software e verificar a existência de novas versões do software ou de pacotes que eliminem os *Backdoors* (esses pacotes de correção são conhecidos como *patches* ou *service packs*.).

Os programas Anti-Vírus não são capazes de descobrir *Backdoors*, somente a atualização dos programas é que podem eliminar em definitivo este problema.

Programas de *Firewall* pessoal, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema.

3.4 Vírus

Vírus de computador são programas capazes de se reproduzir. O ato de se reproduzir, no caso destes Vírus, é a capacidade do mesmo de se copiar de um computador a outro utilizando-se de diversos meios: através dos disquetes, embutindo-se em documentos de texto ou planilhas de cálculo e, atualmente, distribuindo-se por *e-mail*.

3.4.1 Como o computador é infectado por um Vírus?

Seu computador pode ser infectado de diversas maneiras:

- Através de um disquete esquecido no drive A: quando o micro é ligado;
- Executando um programa desconhecido que esteja em um disquete ou, até mesmo, em um CD-ROM;
- Instalando programas de procedência duvidosa;
- Abrindo arquivos do Word, Excel, etc;

- Em alguns casos, abrindo arquivos anexados aos *e-mails*.

É claro que novas maneiras do computador ser infectado por um Vírus podem ser criadas. Neste caso é sempre bom manter-se informado através de jornais, revistas e dos *sites* dos fabricantes de Anti-Vírus.

3.4.2 O que os Vírus podem fazer no computador?

Infelizmente os Vírus podem fazer de tudo, desde mostrar uma mensagem de "feliz aniversário" até destruir irremediavelmente os programas e arquivos de seu computador. Praticamente o vírus passa a ter controle total sobre o computador.

3.4.3 O computador pode ser infectado por um Vírus sem que se perceba?

Sim, sempre. A idéia do Vírus é permanecer escondido (encubado) reproduzindo-se e infectando outros micros até um evento qualquer acordá-lo. Geralmente os Vírus entram em atividade em alguma data específica como na sexta-feira, dia 13.

3.4.4 Como posso saber se o computador está infectado?

Os sistemas operacionais dos computadores (como o Windows ou o MacOS) não detectam Vírus, assim sendo, a melhor maneira de descobrir se um computador está infectado é através dos programas Anti-Vírus.

3.4.5 Existe alguma maneira de proteger o computador dos Vírus?

Sim, instalando e mantendo atualizado um bom programa Anti-Vírus[6] e evitando executar programas desconhecidos. Como medida de prevenção, veja a seção 3.4.1.

3.5 Programas de *E-Mail*

3.5.1 Medidas preventivas no uso dos programas de *E-Mail*

Existem no entanto medidas preventivas que minimizam os problemas trazidos com os *e-mails*:

1. Desligue a opção de "auto-execução" dos programas anexados ao *e-mail*;
2. Desligue a opção de "auto-abertura" dos arquivos anexados aos *e-mails*;
3. Desligue as opções de execução de programas *Java* e do *JavaScript*.

[6] Alguns fabricantes de Anti-Vírus fornecem versões gratuitas para uso pessoal.

Todos estes ítens evitam a propagação automática dos Vírus e Cavalos de Tróia. Alguns programas de *e-mail* não possuem estas opções, neste caso estas funções não estão implementadas, ou seja, o programa de *e-mail* não realizará estas tarefas porque não foi programado para isto.

É claro que se o usuário desligar as opções 1 e 2, mas ainda assim abrir os arquivos ou rodar manualmente os programas que vêm anexados aos *e-mails*, será infectado pelo Vírus (ou Cavalo de Tróia).

Portanto, a regra de ouro é: Não abra arquivos ou programas anexados aos *e-mails* enviados por desconhecidos.

3.6 *Browsers*

Browser é todo e qualquer programa que busca páginas na Internet e as apresentam na tela. Os mais utilizados são o *Netscape Navigator* e o *Internet Explorer*.

3.6.1 Como um *Browser* pode ser perigoso?

De várias maneiras:

- Através de programas *Java*;
- Através de programas *JavaScript*;
- Através de programas ou controles *ActiveX*;
- Através de downloads de programas hostis em sites não confiáveis.

Nos três primeiros casos seu browser sai rodando os programas sozinho sem interferência do usuário, no último caso você tem que baixar o programa da Internet em uma pasta e rodar ou instalar o mesmo.

3.6.2 O que é *Java*?

Java é um jeito de fazer programas, desenvolvido pela empresa Sun Microsystems de modo que o programa feito possa ser utilizado em diversos tipos diferentes de computadores e aparelhos[7].

Na verdade quem "roda" os programas *Java* é um outro programa chamado *Máquina Virtual* Java. Praticamente todos os *browsers* possuem uma máquina virtual dessas embutida[8] e como não existe diferença entre uma máquina virtual de um *browser* para outro, basta fazer uma única versão do programa em *Java*.

Estes programas aparecem dentro das páginas da Internet e podem ser desde simples programinhas de efeitos especiais como pacotes de escritórios completos, com editor de texto, planilha de cálculo, etc. Claro que quanto mais complexo for o programa em *Java*, maior é seu tamanho e mais tempo leva para baixá-lo da rede.

[7] O *Java* foi criado para ser utilizado em aparelhos eletro-domésticos como TV, vídeo, etc. Em um futuro não muito distante será utilizado em relógios de pulso.

[8] Só por curiosidade: existem máquinas virtuais independentes, assim os programas *Java* podem ser rodados sem a necessidade do *browser*.

3.6.3 Um programa *Java* é seguro?

Normalmente sim. As máquinas virtuais dos *browsers* são isoladas do resto do computador, assim um programa *Java* não tem como afetá-lo diretamente[9]. Mas defeitos nestas máquinas virtuais podem fazer com que determinados programas em *Java* (só os hostis) possam causar algum estrago no computador.

3.6.4 Como me protejo de um programa *Java* hostil?

Normalmente as páginas não têm muitos programas em *Java* ou estes não comprometem a sua visualização. Assim sendo, pode-se desligar o *Java* no seu *browser*[10] evitando-se assim maiores dores de cabeça. Claro que se for absolutamente necessário o *Java* estar ligado para que as páginas de um site possam ser vistas (no caso dos *sites* de Home-Banking, por exemplo), basta ligá-lo novamente e entrar no site.

Se você mantiver seu *browser* sempre atualizado não terá grandes dores de cabeça com o *Java* e alguns dos anti-vírus mais atuais possuem a capacidade de detectar os programas *Java* hostis enquanto o *browser* está baixando pela Internet.

3.6.5 O que é *JavaScript*?

Lembra do *Java*? Agora imagine que você quer só colocar um programinha na página para mudar a cor de um desenho quando a setinha do *mouse* passar por cima dele. Pensando nisso, foi criado o *JavaScript*[11].

Curiosidade: o *JavaScript* acompanha a página, ou seja, ele está misturado com os códigos da página e pode ser visto se você pedir para o *browser* mostrar os códigos. Assim, para usar o mesmo programa *JavaScript* em outras páginas o profissional que faz as páginas tem que reescrever o programa em cada uma delas (se usasse *Java*, neste caso, só teria que escrever uma única vez).

3.6.6 Um programa *JavaScript* é seguro?

Como o *JavaScript* é uma versão bem enxuta do *Java* ele normalmente não é capaz de realizar grandes estragos em seu computador, mas valem para ele as mesmas dicas do *Java*.

3.6.7 Como me protejo de um programa *JavaScript*?

JavaScript é muito mais utilizado em páginas do que o *Java*, assim caso você desligue esta opção muitas páginas deixarão de funcionar. Assim, o conselho é

[9] Chamam isso de *Sandbox*, ou caixa-de-areia.

[10] Geralmente tem um botão que desliga o *Java* e o *JavaScript* na parte de Preferências, Configurações ou Opções de seu *browser*.

[11] *JavaScript* pode ser encarado como a versão *diet* do *Java*.

desligar o *JavaScript* quando visitar uma página desconhecida e religá-lo depois, caso seja necessário.

3.6.8 O que é *ActiveX*?

Os programas (ou controles) feitos em *ActiveX* funcionam de maneira similar aos programas feitos em *Java*, mas só podem ser rodados em máquinas com *Windows*. Basicamente estes programas fazem a mesma coisa que os programas *Java* fazem.

3.6.9 O *ActiveX* é seguro?

Diferente dos programas *Java*, os programas *ActiveX* podem fazer de tudo em seu computador, desde enviar um arquivo qualquer pela Internet, até instalar programas em sua máquina.

Antes de baixar um programa *ActiveX* o seu *browser* verifica a procedência do mesmo através de um esquema de certificados digitais[12]. Se você aceitar a certificação o programa será rodado em sua máquina. Se os programas vierem de um site idôneo e você aceitar o certificado do site não haverá grandes problemas.

3.6.10 Como me protejo de um programa *ActiveX*?

Você pode não aceitá-los quando entra em um *site* ou somente aceitá-los de *sites* conhecidos e de boa reputação. Alguns programas de anti-vírus são capazes de identificar e bloquear programas *ActiveX* maliciosos.

3.7 *WebChats*

WebChats são conhecidos por vários nomes, você já deve ter visitado alguns ou pelo menos já ouviu falar deles. *WebChats* são as famosas salas de bate-papo, onde as pessoas entram para jogar conversa fora.

3.7.1 Há perigo em *WebChats?*

Alguns *WebChats* usam *Java* ou *JavaScript* nas suas páginas, assim, valem as dicas do *Java* e do *JavaScript*.

Normalmente o perigo nas salas de bate-papo são as conversas mesmo. Você pode passar seu *e-mail*, endereço, telefone, etc, etc, numa conversa “amigável” e descobrir depois que a pessoa do outro lado é um estelionatário. Lembre-se que você não vê nem ouve as pessoas que estão nas salas. Portanto, tente não se arriscar muito nos bate-papos, evitando passar informações que podem ser utilizadas contra você.

[12] Algo parecido com o reconhecimento de firma nos documentos de cartório.

3.8 Programas de Troca Instantânea de Mensagens

São programas que possibilitam descobrir se uma pessoa está ligada na Internet e, ao mesmo tempo, trocar mensagens, endereços de sites e arquivos com ela. Alguns programas de troca criam salas de bate-papo com diversos tópicos, ou canais, como normalmente são chamados.

Os mais conhecidos são: *ICQ*, *IRC*, *AIM*, etc. Praticamente cada provedor tem o seu próprio programa para troca de mensagens.

3.8.1 Como funcionam os programas de Troca Instantânea de Mensagens?

Basicamente o programa utiliza a Internet para se conectar a um servidor específico. Quando o mesmo se conecta ao servidor ele registra você no banco de dados e verifica quais dos seus amigos estão no ar. A partir daí este programa estará apto a trocar as mensagens. Caso a outra pessoa esteja fora do ar, a mensagem será guardada no servidor e enviada tão logo esta pessoa se conecte.

Normalmente a troca de mensagens e arquivos não passa pelo servidor. Toda vez que a conexão é feita o servidor passa a conhecer o endereço na Internet (endereço IP) do seu computador[13]. Este IP é enviado para os programas de troca de mensagem de seus amigos, assim, como cada um conhece o endereço do outro, as trocas de mensagem ou arquivos não mais necessitarão do servidor.[14]

3.8.2 Os programas de Troca Instantânea de Mensagens são seguros?

Programas de troca de mensagens ficam sempre conectados a um servidor (senão não teriam como saber quem está no ar) e, como estão conectados, podem ser atacados por *hackers*. Não se esqueça que os programas que utilizam a Internet para prestar algum serviço (neste caso troca de mensagens) podem possuir *Backdoors* e ficarem sujeitos a ataques externos.

3.8.3 Como me proteger nos programas de Troca Instantânea de Mensagens?

Valem sempre as mesmas regras básicas. Não aceite arquivos de pessoas desconhecidas, principalmente programas de computadores. Tente evitar fornecer muita informação a pessoas que você acabou de conhecer, como nos WebChats e, principalmente, esconda seu endereço da Internet (endereço IP) quando estiver utilizando este tipo de programa. Os programas de troca de mensagens possuem esta opção em sua configuração e quando acionada a troca das mensagens passa a ocorrer

[13]Toda e qualquer máquina ligada à Internet, por modem, cabo, rádio, fibra-óptica, ou qualquer outro meio, apresenta um endereço único chamado de endereço IP. No caso de provedores, cada vez que você liga para ele, um IP diferente (de uma lista) é fornecido para a sua máquina (IP dinâmico). No caso de servidores, o IP é fixo. Funciona como números de telefone.

[14]Seu programa de troca de mensagens mantém normalmente ativa a conexão para o servidor e outra intermitente para o micro da pessoa para quem você manda as mensagens ou arquivos.

somente pelo servidor (a troca de arquivos normalmente deixa de funcionar neste caso).

Os fornecedores destes programas geralmente mantém páginas na Internet com considerações a respeito de segurança e o que fazer para se proteger melhor. Vale a pena gastar uns minutinhos de seu tempo para ler estas páginas ou ler dicas de utilização nas revistas especializadas em informática. A cada nova versão destes programas, mais recursos são introduzidos, mudando os aspectos de segurança, assim, o negócio é ficar sempre de olho nestes sites, nas revistas especializadas e nos cadernos de informática dos jornais para verificar se as opções de segurança dos programas foram alteradas, assim como dicas de utilização.

O caso do *IRC* é mais complicado, como o programa é mais complexo, possui um grande número de comandos e tem várias salas de bate-papo (no *IRC* são chamados de canais), fica difícil pensar em segurança. Por exemplo: existe a possibilidade de o usuário do *IRC*, sem querer, tornar disponível o acesso ao disco rígido (drive `C:`) de seu computador, possibilitando aos outros usuários do *IRC* roubarem a sua senha do provedor ou outros dados importantes. O *IRC* é um programa muito utilizado por *hackers* para troca de informações e arquivos, por isso, todo cuidado é pouco.

3.9 Programas de Distribuição de Arquivos

Arquivos podem ser enviados (*upload*) ou recebidos (*download*) por uma infinidade de maneiras diferentes: através do e-mail, através dos programas de mensagem instantânea (ICQ, entre outros) e mesmo através dos *browsers*. Mas, diferente destes, existem os programas construídos com a única finalidade de facilitar a troca de determinados tipos de arquivos entre os usuários, como é o caso do Napster (que troca arquivos de música do tipo MP3) e o atual Gnutella (que troca todo e qualquer tipo de arquivo).

3.9.1 Como funcionam os programas de Distribuição de Arquivos?

Estes programas funcionam da seguinte maneira: quando o programa é conectado ao servidor ele envia uma lista dos arquivos que estão em uma pasta específica (já pré-configurada na instalação do programa) de seu computador e esta lista fica disponível para os demais usuários do programa no mundo todo.

Quando você busca por um arquivo (música por exemplo) o programa pergunta ao servidor quais computadores possuem aquele arquivo, quando você escolhe um dos arquivos o programa que está rodando em sua máquina se conectará ao programa da outra pessoa e baixará o arquivo escolhido para alguma pasta de seu computador (já pré-configurada e, normalmente, diferente da pasta anterior).

Assim o único trabalho do servidor é manter uma lista de quais computadores estão no ar (conectados à internet e rodando o programa de distribuição de arquivos) e a lista dos arquivos disponíveis. O trabalho de baixar os arquivos e enviar os arquivos para seus amigos (quando eles pedem o arquivo) é de seu computador.

3.9.2 Os programas de Distribuição de Arquivos são seguros?

Imagine a seguinte situação, se você sem querer altera a configuração de um programa desses e coloca como pasta de distribuição (aquela onde você coloca os arquivos para distribuição) uma pasta com informações confidenciais a seu respeito ou na pasta `C:\Windows` onde ficam guardadas as suas senhas, com o Napster você não iria ter grandes problemas visto que ele só trata de programas de música, mas no caso do Gnutella, automaticamente todos os arquivos estarão disponíveis.

Dificilmente arquivos de música, foto ou vídeo apresentarão problemas, a dificuldade maior será com os arquivos de programas que poderão conter Vírus ou Cavalo de Tróia embutidos. Vale a mesma regra dos casos anteriores, evite baixar da rede programas de desconhecidos.

3.9.3 Como me proteger usando programas de Distribuição de Arquivos?

Valem sempre as mesmas regras: sempre desconfie de programas ou arquivos de desconhecidos, pois eles podem conter vírus ou cavalos-de-tróia. Tenha um bom anti-vírus em seu computador e mantenha-o atualizado sempre.

4 Privacidade

4.1 Privacidade nas visitas aos sites

Você já deve ter percebido que quando entra em determinados *sites* aparecem na página dados de seu computador que às vezes até assustam. Parecem adivinhar até a cor do papel-de-parede que você está utilizando em seu computador.

Isto ocorre porque existe um bate-papo entre o seu *browser* e o *site* que você está visitando. Entre as informações que seu *browser* entrega de bandeja para o servidor do *site* visitado estão:

- O endereço na Internet de seu computador (endereço IP);
- Nome e versão do sistema operacional;
- Nome e versão do *browser*;
- Última página visitada;
- Resolução do monitor.

Com estas informações os *sites* conseguem fazer as estatísticas de visitação, adequar à página do *site* ao *browser* do usuário, etc.

Seu *browser* sempre passará estas informações aos *sites* visitados. Se você quer realmente se esconder (ficar anônimo) e não passar nenhuma informação ao *site* visitado deverá se utilizar de serviços como o do *Anonymizer* (`http://www.anonymizer.com`).

4.1.1 O que são *Cookies*?

Cookies são pequenas informações, deixadas pelos *sites* que você visita, em seu *browser*. Os *Cookies* são utilizados pelos *sites* de diversas formas, eis algumas:

- Para guardar a sua identificação e senha quando você pula de uma página para outra;
- Para manter uma "lista de compras" em sites de comércio eletrônico;
- Personalização de *sites* pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas destes *sites*;
- Manter alvos de *marketing*, como quando você entra em um site de CDs e pede somente CDs de MPB, e depois de um tempo você percebe que as promoções que aparecem são sempre de CDs de MPB (as que você mais gosta);
- Manter a lista das páginas vistas em um *site*, para estatística ou para retirar as páginas que você não tem interesse dos *links*.

O problema com relação aos *Cookies* é que eles são utilizados por empresas que vasculham suas preferências de compras e espalham estas informações para outros *sites* de comércio eletrônico. Assim você sempre terá páginas de promoções ou publicidade, nos sites de comércio eletrônico, dos produtos de seu interesse. Na verdade não se trata de um problema de segurança, mas alguns usuários podem considerar este tipo de atitude uma **invasão de privacidade**.

Os *browsers* possuem opções que desligam totalmente o recebimento de *Cookies*, limitam o trânsito dos mesmos entre seu *browser* e os *sites* visitados ou opções que fazem com que seu *browser* peça uma confirmação ao usuário toda vez que recebe um *cookie*. Alguns *browsers* possibilitam ver o conteúdo dos *Cookies*.

4.2 Privacidade dos e-mails

Todos os provedores são capazes de ler as correspondências eletrônicas de seus usuários, sempre. Esta notícia geralmente cai como uma bomba. Por mais que os provedores possam negar, os *e-mails* ficam a disposição do administrador dos servidores. Existe, no entanto, um consenso ético de o provedor nunca "olhar" o conteúdo das caixas-postais dos usuários sem o consentimento dos mesmos.

O sistema de envio e recebimento de *e-mails* foi criado, na década de 70, visando a troca de mensagens simples e curtas entre duas pessoas. A partir daí este serviço cresceu assustadoramente, mas manteve a simplicidade original. O problema desse sistema é que foi comparado com o correio terrestre normal (se bem que um carteiro qualquer poderia ler seus cartões-postais), dando a falsa idéia de que os *e-mails* são confidenciais.

As mensagens que chegam em sua caixa postal ficam armazenadas em um arquivo no servidor até você se conectar na Internet e baixar os *e-mails* através do seu

programa de *e-mails*. Portanto, enquanto os *e-mails* estiverem no servidor ou em trânsito eles poderão ser lidos pelos administradores dos servidores do provedor.

Se a informação que se deseja enviar por *e-mail* for confidencial a solução é a utilização de programas de criptografia que "trancam" o *e-mail* através de chaves (senhas ou frases) e que so podem ser "destrancados" por quem possuir a chave certa para isso. Alguns programas de criptografia já podem estar embutidos nos programas de *e-mails* ou podem ser adquiridos separadamente e serem anexados aos programas de *e-mails*. Prefira no caso os programas de criptografia que trabalham com pares de chaves, vide seção 5.3.

4.3 *SPAM*

Muitos de nós já devem ter recebido pelo menos um *SPAM*. Estas são as famosas mensagens de *e-mails* não solicitadas e que entulham nossas caixas-postais de baboseiras. O *SPAM* não é oficialmente proibido, mas considera-se, na Internet, uma falta de ética descabida.

Existem organizações não governamentais que matém listas de domínios[15] neste contexto (domínios são os nomes que aparecem depois do @ no endereço de *e-mail*) que sempre são origem de *SPAM*. Seu provedor pode, ou não, dependendo da política adotada, configurar o sistema de recebimento de *e-mails* para bloquear os *e-mails* vindos dos domínios destas listas.

4.4 *HOAX*

Hoaxes[16] são comuns na Internet e são *e-mails* que possuem conteúdos alarmantes ou falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais. Em geral se você ler atentamente estes *e-mails* notará que seus conteúdos são absurdos sem sentido. Essas mensagens podem estar acompanhadas de vírus.

Dentre os *hoaxes* típicos temos as correntes ou pirâmides, pessoas ou crianças que estão prestes a morrer de câncer, etc. Histórias deste tipo são criadas para espalhar desinformação pela Internet.

Este tipo de *e-mail* foi inventado para entupir as caixas postais dos grandes provedores. Outro objetivo de quem escreve este tipo de mensagem é verificar o quanto ela se espalha pelo mundo e por quanto tempo ela continua a ser espalhada, mais ou menos os objetivos de quem programa Vírus. Estas mensagens se propagam tanto pela boa vontade e solidariedade de quem as recebe e, por isso, é praticamente impossível eliminá-las da Internet.

Quem repassa este tipo de mensagem para os amigos ou conhecidos acaba endossando ou avalizando indiretamente o que está escrito, e as pessoas que recebem os *e-mails* de você acabam confiando em sua pessoa e não verificam a procedência nem a veracidade da história.

[15] Dentre eles o `http://maps.vix.com/`.

[16] Boatos.

Neste endereço, http://HoaxBusters.ciac.org/ você encontra uma lista de *hoaxes* que estão circulando pela Internet com seus respectivos textos.

4.5 Seus dados pessoais!

Jamais entregue seus dados pessoais (nome, e-mail, endereço, números de documentos e, principalmente, número de cartão de crédito) em qualquer site que você visita. Não se esqueça que estas informações são guardadas em algum banco de dados do site e podem ser vendidas (o que seria anti-ético) para outras empresas. Seu e-mail pode ser utilizado em alguma lista de distribuição de *SPAMs*.

4.6 Formulários, Comércio Eletrônico e *Home-Banking*

Sempre que utilizar a internet para transações comerciais envolvendo seu dinheiro, verifique dois ítens importantíssimos.

- Se o *site* visitado pertence a uma instituição de confiança e tem bom nome no mercado;
- Se o *site* utiliza algum esquema de conexão segura[17].

O primeiro item deve ser óbvio ao usuário, *sites* desconhecidos podem causar mais aborrecimentos do que soluções.

O segundo item é o mais importante no caso, pois garante que os dados digitados nos formulários (ou na realização das transações bancárias, por exemplo) estejam protegidos dos olhares curiosos dos *hackers*.

Como verificar, então, se a conexão é segura? Existem duas maneiras diferentes, primeiro através do endereço do *site* que deve começar com `https://` (diferente dos `http://` das conexões normais), o **s** antes do sinal de dois-pontos indica que o endereço em questão é de um *site* com conexão segura e, portanto, os dados do formulário serão criptografados (vide seção 5.3) antes de serem enviados.

Outra indicação, e a mais importante, é que o seu *browser* irá indicar se a conexão está segura através de algum sinal. O sinal mais adotado nos *browsers* é o de um desenho de um **cadeadinho fechado** (se o cadeado estiver aberto, a conexão não é segura). Se você clicar em cima deste cadeado você obterá informações sobre o método de criptografia utilizado para cifrar os dados do formulário (ou da transação), verifique sempre o tamanho da chave utilizada, chaves menores que 40bits, que são usadas em *browsers* mais antigos, são consideradas inseguras, o ideal é utilizar *browsers* que usem chaves de pelo menos 128bits de tamanho (as versões mais atuais dos *browsers* já utilizam chaves deste tamanho).

As transações comerciais via Internet são tão seguras quanto as realizadas "no balcão", somente verifique se a conexão está segura antes enviar qualquer dado ao *site*.

[17] No caso, chamado de SSL (*Secure Socket Layer*).

5 Programas para a Proteção do Usuário

5.1 Anti-Vírus

Os anti-vírus são programas que detectam, anulam e eliminam os vírus de computador. Atualmente os programas anti-vírus foram ganhando novas funcionalidades e conseguem eliminar *Cavalos de Tróia*, barram programas *Java* e *ActiveX* hostis e verificam *e-mails*.

Um bom anti-vírus deve possuir as sequintes funcionalidades:

- Identificar e eliminar uma boa quantidade[18] de vírus;
- Analisar os arquivos que estão sendo baixados pela internet;
- Verificar continuamente os discos rígidos e flexíveis (Drives C: e A:) de forma transparente ao usuário;
- Procurar vírus e *Cavalos de Tróia* em arquivos anexados aos *e-mails*;
- Criar um disquete de verificação (disquete de *boot*) que pode ser utilizado caso o vírus seja mais esperto e anule o anti-vírus que está instalado no computador;
- Atualizar os bancos de dados de vírus pela rede.

Alguns anti-vírus, além das funcionalidades acima, ainda verificam o funcionamento dos programas de seu computador, avisando ao usuário; caso algum programa comece a apresentar algum comportamento suspeito[19] (como por exemplo, o programa de *e-mail* começar a mandar *e-mails* sozinho).

As dicas para o uso do anti-vírus são simples: mantê-lo sempre atualizado e criar o disquete de verificação para utilizá-lo de vez em quando ou quando seu computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco C: fora de hora, etc.). É importante passar manualmente o anti-vírus em todo e qualquer disquete que esteja no drive A:.

Algumas versões de anti-vírus são gratuitas para uso pessoal e podem ser baixadas pela Internet.

5.2 Firewalls

Os *Firewalls* são sistemas ou programas que barram conexões indesejadas na Internet. Assim, se algum *hacker* ou programa suspeito tenta fazer uma conexão ao seu computador o *firewall* irá bloquear. Com um *firewall* instalado em seu computador, grande parte dos *cavalos de tróia* serão barrados mesmo se já estiverem instalados em seu computador.

[18]Existem cerca de 50.000 tipos de vírus

[19]Isto é feito com técnicas de inteligência artificial.

Alguns programas de *firewall* chegam ao requinte de analisar continuamente o conteúdo das conexões, filtrando os *cavalos de tróia* e os vírus de *e-mail* antes mesmo que os anti-vírus entrem em ação. Esta análise do conteúdo da conexão serve, ainda, para os usuários barrarem o acesso a *sites* com conteúdo erótico ou ofensivo, por exemplo.

Existem, ainda, pacotes de *firewall* que funcionam em conjunto com os anti-vírus possibilitando ainda um nível maior de segurança nos computadores que são utilizados em conexões com a Internet.

Assim como certos anti-vírus, alguns fabricantes de *firewalls* oferecem versões gratuitas de seus produtos para uso pessoal. Existem programas e sistemas de *firewall* extremamente complexos que fazem uma análise mais detalhada das conexões entre os computadores e que são utilizados em redes de maior porte e que são muito caros para o usuário doméstico. A versão doméstica deste programa geralmente é chamada de *firewall pessoal*.

Normalmente estes programas de *firewall* criam arquivos especiais em seu computador denominados de arquivos de *log*. Nestes arquivos serão armazenadas as tentativas de invasão que o *firewall* conseguiu detectar e que são avisadas ao usuário. Caso necessário envie este arquivo de *log* para seu provedor, assim o pessoal do provedor poderá comparar os seus *logs* com os do provedor, verificando se a **invasão** ocorreu de fato ou foi um alarme falso[20].

5.3 Criptografia e Assinatura Eletrônica de Documentos

Criptografia é a arte e a ciência de criar mensagens que possuem combinações das seguintes características: ser privada, somente quem enviou e quem recebeu a mensagem poderá lê-la; ser assinada, a pessoa que recebe a mensagem pode verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de repudiar qualquer mensagem que possa ter sido modificada. Os programas de criptografia disponíveis no mercado, para criptografia de mensagem de *e-mails*, normalmente possuem todas estas características.

Um método de criptografia de texto utilizado por Júlio Cesar para se comunicar com suas tropas é conhecido atualmente por Rot13[21], que consistia em trocar as letras das palavras por outras (13 letras distantes), assim A seria trocado por O, B por P e assim por diante (Z seria trocado por M). Para obter o texto original basta destrocar as letras. É claro que atualmente existem “receitas[22]” de criptografia muito mais complicadas e poderosas do que esta.

As “receitas” de criptografia atuais utilizam o que chamamos de “chave” para cifrar e decifrar uma mensagem. Esta chave é uma seqüência de caracteres, como

[20]Os *firewalls* baseiam-se em regras genéricas de verificação e, infelizmente, geram muitos avisos falsos. Por isso a necessidade de se comparar com os *logs* do provedor.

[21]Qualquer computador atual quebra esse tipo de criptografia num piscar de olhos.

[22]Em informatiquês as “receitas” são chamadas de algorítmos. Um programa de computador é, portanto, um conjunto de algorítmos que realizam alguma tarefa.

sua senha, que são convertidos em um número[23]. Este número é utilizado pelos programas de criptografia para cifrar sua mensagem e é medido em *bits*, quanto maior o tamanho da chave, mais caracteres (letras, números e sinais) devem ser utilizados para criá-la[24].

5.3.1 Criptografia de Chave Única

Quando um sistema de criptografia utiliza chave única quer dizer que a mesma chave que cifra a mensagem serve para decifrá-la. Isto quer dizer que para você e seus amigos poderem trocar mensagens cifradas todos deverão utilizar a mesma chave. É claro que se você se corresponder (trocar *e-mails*) com um grande número de pessoas a sua chave perderá a utilidade pois todos a conhecerão, portanto, estes métodos são mais úteis para cifrar documentos que estejam em seu computador do que para enviar mensagens para amigos.

Os métodos de criptografia por chave simples são rápidos e difíceis de decifrar. As chaves consideradas seguras para este tipo de método de criptografia devem ter pelo menos 128 bits de comprimento.

5.3.2 Criptografia de Chaves Pública e Privada e Assinatura Eletrônica de Documentos

Este tipo de método de criptografia utiliza duas chaves diferentes para cifrar e decifrar suas mensagens. Eis como funciona: com uma chave você consegue cifrar e com a outra você consegue decifrar a mensagem. Qual a utilidade de se ter duas chaves então? Ora, se você distribuir uma delas (a chave "pública") para seus amigos eles poderão cifrar as mensagens com ela, e como somente a sua outra chave (a chave "privada") consegue decifrar, somente você poderá ler a mensagem.

Este método funciona ao contrário também, se você usa a sua chave privada para cifrar a mensagem, a chave pública consegue decifrá-la. Parece inútil mas serve para implementar um outro tipo de serviço em suas mensagens (ou documentos): a Assinatura Eletrônica.

A assinatura eletrônica funciona da seguinte maneira: o texto de sua mensagem é verificado e nesta verificação é gerado um número[25] (este número é calculado de tal forma que se apenas uma letra do texto for mudada, pelo menos 50% dos dígitos do número mudam também), este número será enviado junto com a sua mensagem mas será cifrado com sua chave privada. Quem receber a mensagem e possuir sua chave pública vai verificar o texto da mensagem novamente e gerar um outro número. Se este número for igual ao que acompanha a mensagem, então

---

[23] Para o computador um texto é uma lista de números, claro que cada número representa uma letra ou caracter.

[24] Alguns exigem chaves tão grandes que normalmente são chamadas de *passphrases*. Os *passwords* também podem ser considerados chaves.

[25] São conhecidos por algoritmos de *digest* o mais simples conhecido é somar o valor numérico de cada letra da sua mensagem e usar este número. Por exemplo: aqueles 2 dígitos (dígitos verificadores) que aparecem no fim do CIC são gerados por um *digest*.

pessoa que enviou o *e-mail* será mesmo quem diz ser. Ainda, se alguém mudar algo na mensagem os números não serão mais iguais mostrando que a mensagem foi modificada por alguém.

Lembre-se que suas mensagens de *e-mail* poderão ser somente cifradas, somente assinadas ou cifradas e assinadas ao mesmo tempo. As duas operações são independentes.

Estes métodos de criptografia, no entanto, apresentam dois problemas. São muito mais lentos que os métodos de chave única e as chaves pública e privadas têm que ser muito maiores. Uma chave segura (difícil de ser descoberta) neste caso deve medir pelo menos 512 bits[26].

O método de chave pública e privada mais conhecido é o PGP[27] (existem versões gratuitas na Internet) que adiciona estas funcionalidades ao seu programa de *e-mail*.

Só por curiosidade, a Casa Branca utiliza este tipo de programa para a troca de mensagens entre o presidente e os seus assessores.

5.3.3 Quão segura é a "receita" de criptografia?

Sabemos que por mais poderosa que seja a receita de criptografia ainda assim ela pode ser decifrada. O importante é saber em quanto tempo isto pode ocorrer, por exemplo, no caso de métodos de chave única, se utilizarmos chaves de 40 bits em alguns dias a mensagem pode ser decifrada (testando todas as 2^{40} chaves possíveis[28]). Se utilizarmos chaves de 128 bits (2^{128} de chaves possíveis[29]) um super-computador demoraria alguns milhões de anos.

Este é o caso de se testar todas as chaves possíveis, é claro que podem ter falhas na receita da criptografia, mas as receitas que estão no mercado foram bem testadas e a complexidade de algumas delas garantem a segurança do método. Normalmente as quebras das chaves são realizadas por força-bruta mesmo, testando uma por uma até descobrir a chave utilizada.

6 Fui atacado e agora?

Toda vez que você se sentir lesado, seja por ataques, seja por *e-mail* não solicitado, entre em contato com seu provedor. Todos os bons provedores possuem uma equipe para cuidar da segurança de seus usuários e do próprio provedor. Segundo normas da internet (RFC2142), todos os provedores (domínios[30]) devem possuir os seguintes endereços de *e-mails*:

[26]São usadas chaves de 1024 bits normalmente, militares usam 2048 e paranóicos utilizam chaves de 4192 bits.

[27]*Pretty Good Privacy*.

[28]Isto é igual a 1.099.511.627.776 de chaves diferentes.

[29]Isto é igual a 340.282.366.920.938.463.463.374.607.431.768.211.456 de chaves diferentes.

[30]Um domínio normalmente é o que vem depois do @ no endereço de *e-mail*.

abuse@(seu provedor).com.br Usado para informar a respeito dos *SPAMs* ou *e-mails* de conteúdo abusivo ou ofensivo;

noc@(seu provedor).com.br Utilizado para relatar problemas com a rede; e

security@(seu provedor).com.br Utilizado para relatar problemas envolvendo segurança, como invasões, ataques, etc.

Todos os bons provedores costumam auxiliar o usuário quando este é atacado ou invadido por *hackers*.